AFFIDAVIT

I, Jarred A. Payne, am a Task Force Officer ("TFO") with the Federal Bureau of Investigation ("FBI") being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a law enforcement officer with the Kanawha County, West Virginia Sheriff's Office since February 2017. Prior to that, from 2009 to 2017, I was employed by the Dunbar Police Department. From 2009 to 2014, I was employed as a Patrolman and Corporal. From 2014 to 2017, I was assigned to the Kanawha Bureau of Investigation as a Detective where I investigated major crimes and cybercrimes. I am currently assigned to the FBI as a Task Force Officer. While assigned to the FBI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at FBI's Child Exploitation Unit, the United States Secret Service's National Computer Forensics Institute, the National White Collar Crime Center, Fox Valley Technical College, the West Virginia State Police Academy, and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child

pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have investigated hundreds of cases involving child pornography and child exploitation both in the State of West Virginia and through various Federal investigations. I am a certified Digital Evidence Extraction Technician (DEXT) and Computer Analysis Response Team (CART) Technician through the FBI and received specialized training and certification through the FBI for those, both in Quantico, Virginia. Moreover, I am a deputized federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. § 2423, and I am authorized by law to request a search warrant.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of the following property as further described below and in Attachment A: (1) Google Pixel 6 Pro cell phone, IMEI #358339778746149, (2) Google Pixel 3 XL cell phone, IMEI #357406100004082, (3) Samsung SM-T530NU tablet, Serial Number #R52FA17LV3N, and 16 GB MicroSD memory card contained therein, and (4) a 128 GB unlabeled flash drive (collectively "the Devices") and the extraction from the Devices of electronically stored information in order to seize the items described in Attachment B. The Devices are currently in law enforcement possession in Charleston, Kanawha County, West Virginia.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The probable cause statement is based upon information of which I am personally aware as well as information that has been conveyed to me by other law enforcement officers.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched includes the contents of four electronic devices ("the Devices"): (1) a Google Pixel 6 Pro cell phone, IMEI #358339778746149, with black case, (2) a Google Pixel 3 XL cell phone, IMEI #357406100004082, (3) a Samsung SM-T530NU tablet, Serial Number #R52FA17LV3N, and the 16 GB MicroSD memory card contained therein, with black case, and (4) a 128 GB unlabeled flash drive, black in color.

5. The Devices are presently in the possession of the FBI, located locally at 113 Virginia Street East, Charleston, WV 25301. The Devices were lawfully seized from Jerrod Lee Sharp's ("SHARP") person and accompanying luggage on July 30, 2023, pursuant to arrest and/or as part of an inventory search of his luggage. Upon information and belief, the Devices have been maintained in such a manner that they are in the same condition as at the time they were seized.

6. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

7. SHARP is currently under indictment for violations of Title 18, United States Code, Sections 2422(b) (attempted enticement of a minor) and 2423(b) and (e) (travel to engage in illicit sexual activity with a minor). Additional evidence provides probable cause to believe that SHARP committed offenses under 18 U.S.C. § 2252A (possessing, receiving, and distributing child pornography). I seek to search the Devices to locate evidence of criminal violations set forth above for items specified in Attachment B, incorporated herein by reference.

PROBABLE CAUSE

8. A law enforcement officer acting in an undercover capacity ("UCO") created a profile on a fetish website. The UCO was portraying a mother of two girls, ages 11 and 13, living in the Beckley, Raleigh County, West Virginia area. On or about August 18, 2022, the UCO was contacted by a user on the fetish website who was later identified as JERROD LEE SHARP, age 39, of Ponca City, Kay County, Oklahoma.

9. In his initial messages to the UCO, SHARP stated that he "was always wanting to have a little fun" and wanted to "learn more about momma bear and her cubs." The UCO advised SHARP at that time that she had two daughters, ages 11 and 13.

10. On August 18, 2022, the conversation moved from the fetish website to text message. In their first conversation, SHARP explained that he "want[ed] to have a family that is sexually active with each other" and "are open sexually" when anyone wants to have sex and indicated that he was interested in such a family with the woman and her children.

11. On August 20, 2022, SHARP asked if the UCO had Wickr because he "could send [her] some fun photos there safely." Wickr is a messaging application that can be accessed by computer or a cell phone application. The application allows users to send messages and media (including images and videos) via secure, end-to-end encrypted messages. End-to-end encryption involves the encryption of a message on the sender's device and decryption of the message on the recipient's device; the Wickr platform itself is unable to review or access the content of messages sent via the platform. Wickr also allows users to create anonymous accounts without providing any identifying information, such as email addresses or phone numbers. Messages sent via Wickr also disappear after a set amount of time.

12. By August 30, 2022, SHARP mentioned that he "could definitely drive up and see" the woman and her children. During that conversation, SHARP began discussing his sexual preferences with the girls, explaining that he "would rather be very careful" than put the girls on birth control. He advised that "it would be

best to find a sympathetic midwife or maternity nurse" if one of them got pregnant, "but with proper timing it would be very unlikely[.]"

13. On September 13, 2022, SHARP again mentioned that he wanted to come visit them in a month or so. SHARP explained the family bonding he desired: "Imagine both the girls kneeling next to us sucking and licking your nipples as you bounce up and down on Father's nice thick cock. An[sic] while they use their mouths on you Daddy's hands are under each of them rubbing where they need the most physical bonding…." A few days later, SHARP noted that he would "cherish" the 11-year-old's virginity if she gave it to him. SHARP proceeded to explain in graphic detail how he wanted to take her virginity:

> I would want you and her sister to lick, and kiss, and tease her all over until she is excited and ready. Then I'll walk up and you three can use your mouth on me to make sure I'm ready also (I doubt that will be any problem with three beautiful girls) then I will lay down and you will get to guide your daughter's hips down onto my cock. You will straddle me facing her and kiss her as her sister teases her body from behind.

14. On November 5, 2022, after several months of speaking almost daily to the UCO, SHARP asked the UCO what airport was closest to them. SHARP later revealed that driving might be better so that he could bring all of his "toys," namely a "hitachi" (presumably a type of vibrator) and a "sybian" (presumably a

reference to a "Sybian saddle," which is a saddle-like vibrator and sex toy for women).

15. On January 1, 2023, SHARP began emailing the girls directly. He told the 11-year-old that he wanted to be her new "daddy" and that he would be coming to "play" with her. He also told her that she "will get to be the center of [his] attention" and called her "My Little Darling."

16. SHARP informed the 11-year-old girl that he would make sex "as painless as I can make it" but that "the first time some times can come with a bit of pain or discomfort." SHARP told the 11-year-old girl that they can "slow down or go very shallow" until she feels better, and he promised to "do all I can to help you enjoy it."

17. SHARP also emailed the 13-year-old, instructing her to not scare her 11-year-old sister about sex hurting and that he would "minimize any pain [the 11-year-old] feels."

18. SHARP spoke on the phone with the UCO several times beginning in March of 2023. The phone conversations, like the text messages, were focused on SHARP's interest in traveling to West Virginia to meet the girls and engage in sexual intercourse with them, ultimately creating a sexually active family unit.

19. On April 14, 2023, SHARP again explicitly detailed what he was seeking with the UCO and her girls via text message:

> So, I will just be plain with you about what I want. I am a poly amorous person. I also have been into the BDSM lifestyle for a long time. I want a permanent relationship with you. I want a permanent relationship with your daughters. I want you to call me your Man and I want them to call me Father. I want more than a regular family situation though. While we will obviously be having sex, I want to have sex with both [girls] also. They will have access to my body at all times just like you would, and I would have access to all of you. I want to not only have you watch while I play with them but I will eventually have you join in. I would like to have times where someone's stressful day gets washed away by all of us laying that person down and pleasing them.

20. That same date, SHARP asked whether or not the UCO had an Apple cell phone because "Apple has began scanning photos on iPhone's for child material."

21. On several occasions in May of 2023, SHARP asked for whatever pictures of the girls that the UCO felt comfortable sending.

22. On June 27, 2023, SHARP discussed a phone that he was planning to send the UCO. He noted, "it will be completely locked down and safe to say or send whatever you want on it."

23. In July 2023, SHARP booked a flight from Oklahoma to Yeager Airport in Charleston, West Virginia, with a scheduled arrival of July 30, 2023. He told the UCO that he intended to engage in sexual activity with both girls during the trip. SHARP advised the UCO that he was going to check his luggage bag rather than carry it on so that he could pack sex toys. They discussed

how the UCO was to pick SHARP up from the airport and then drive SHARP back to her home in Beckley, West Virginia.

24. On July 5, 2023, SHARP asked when the girls' birthdays were. The UCO advised that the 13-year-old's was July 26th and the 11-year-old's was August 9th. SHARP asked, "if I send money to that address you gave me will they be able to get it for their birthdays?" That same date, he said to the UCO, "I want you to be comfortable sending me pictures and letting them chat and call me."

25. On July 18, 2023, SHARP sent the UCO credit card information. SHARP instructed the UCO to pay her internet bill with that card if she was ever short on cash for the month. He advised that they needed "to go over every detail" and he wanted to "talk with [her] and the girls consistently until the trip and exchange more pictures of each other."

26. On July 22, 2023, SHARP began a conversation with the UCO on Kik. He provided explicit detail about the sexual acts he wanted to perform with the girls.

27. SHARP described that the 11-year-old girl's "first time will be at her own pace though and each time I cum I will last longer and longer with them."

28. SHARP sent a photograph of his genitals to the UCO and asked if the UCO would "show [her] girls or make them wait."

29. On a July 23, 2023, phone call, SHARP spoke with the UCO and her girls together. The UCO told SHARP that she showed her girls the picture of his genitals that he had sent. SHARP asked if the girls liked it. The 11-year-old said that after seeing it, she was afraid that it would hurt when they played. SHARP assured the 11-year-old that she would enjoy playing and that he might let her "get on top" the first time so that she could go at her own pace.

30. The conversations between the UCO and SHARP continued consistently from August 2022 through July 2023 across text messages, emails, phone calls, and Kik messages. During this time frame, the conversation remained focused on SHARP's interest in traveling to West Virginia to meet the girls and engage in sexual intercourse with them, ultimately creating a sexually active family unit. SHARP also discussed having the UCO and her daughters move to Oklahoma to live with him. On numerous occasions he assured the UCO that this was not a fantasy or role-play.

31. On July 30, 2023, SHARP flew from Oklahoma to Charleston, West Virginia. SHARP met the UCO at the airport and retrieved his luggage from baggage claim. While leaving the airport with the UCO, SHARP was placed under arrest. At the time of his arrest, the Devices were seized as part of a search incident to arrest and an inventory search of his luggage. Since that time, the data on

the Devices has been preserved and the contents of the Devices have not been reviewed by law enforcement.

CHARACTERISTICS OF CHILD PORNOGRAPHY COLLECTORS

32. Based on my experience, I am aware that the following characteristics are common to individuals who trade in child pornography:

a. Individuals who possess and/or distribute child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity, sexually suggestive poses, or from literature describing such activity;

b. Individuals who possess, and/or distribute child pornography may collect sexually explicit or sexually suggestive material depicting children, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. These individuals often maintain this material for sexual arousal and gratification. Furthermore, they may use this material to lower the inhibitions of children they are attempting to seduce, to arouse a child partner, or to demonstrate the desired sexual acts;

c. Individuals who possess, and/or distribute child pornography often possess and maintain copies of child pornographic material, including but not limited to pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, and tape recordings, in the privacy and security of their home. Prior investigations into these offenses have shown that child pornography offenders typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years;

d. Individuals who possess, and/or distribute child pornography often begin their child pornography collections by obtaining child abuse material through various free avenues afforded by the Internet, like P2P

file sharing. Thereafter, these individuals may escalate their activities by producing and/or distributing child pornography, for the purpose of trading this material to add to their own child pornography collection;

e. Individuals who possess, and/or distribute child pornography often maintain their digital or electronic collections in a safe, secure and private environment, such as a computer, Smartphone or surrounding area. These collections are often maintained for several years and are maintained on multiple devices, to afford immediate access to view the material;

f. Individuals who possess, and/or distribute child pornography may correspond with others to share information and material, and rarely destroy this correspondence. These individuals often maintain lists of names, email addresses and telephone numbers of others with whom they have been in contact regarding their shared interests in child pornography.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER AND ELECTRONIC DEVICE SYSTEMS

33. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers and other electronic devices, I know that data can be stored on a variety of computer systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage.

34. As is the case with most digital technology, communications by way of computer or cellular phone can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used.

35. I submit that there is probable cause to believe the items in Attachment B will be stored on the Devices for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are

overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

36. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner.

d. Moreover, information stored within a computer and other electronic storage media may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information within the device may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the device or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

e. A person with appropriate familiarity with how a computer or electronic device system works can, after examining this forensic evidence in its proper context, draw conclusions about how the device was used, the purpose of its use, who used it, and when.

f. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer or electronic device system evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data

stored on such a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

g. Further, in finding evidence of how a computer or electronic device system was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

h. I know that when an individual uses a computer or electronic device system to distribute or attempt to distribute child pornography, the individual's device will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The device is also likely to be a storage medium for evidence of a crime. From my training and experience, I believe that a device used to commit a crime of this type may contain: data that is evidence of how the device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

FORENSIC ANALYSIS

37. Based on the foregoing, and consistent with Federal Rule of Criminal Procedure 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence

described by the warrant. If the Devices have been locked using a passcode, the examination may also include the use of computer programs or other devices to bypass the passcode or otherwise access the material located on the Devices.

38. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

39. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

40. Moreover, I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, unless otherwise ordered by the Court, the return will not include the specific evidence later examined by a forensic analyst.

Further your Affiant sayeth naught.

DETECTIVE JARRED PAYNE
KANAWHA COUNTY SHERIFF'S OFFICE

Sworn to by the Affiant telephonically in accordance with the procedures of Rule 4.1 this 8th day of August, 2023.

Omar J. Aboulhosn
United States Magistrate Judge